## We claim:

1. A method of cryptographic processing on a computer, which comprises the steps of:

prescribing an elliptic curve in a first form, the elliptic curve having a plurality of first parameters;

transforming the elliptic curve into a second form

$$y^2 = x^3 + c^4 a x + c^6 b$$

by determining a plurality of second parameters, wherein at least one of the second parameters is shortened in length by comparison with the first parameter;

wherein x,y are variables;

a,b are the first parameters; and

c is a constant;

wherein at least the parameter a is shortened by selecting the constant c such that

c⁴a mod p

is determined to be significantly shorter than a length of the parameter b and the length of the prescribed variable p; and

determining the elliptic curve in the second form for cryptographic processing.

- 2. The method according to claim 1, wherein the first form of the elliptic curve is defined by  $y^2 = x^3 + ax + b$ .
- 3. The method according to claim 1, which comprises carrying out cryptographic encoding.
- 4. The method according to claim 1, which comprises carrying out cryptographic decoding.
- 5. The method according to claim 1, which comprises carrying out key allocation.
- 6. The method according to claim 1, which comprises carrying out a digital signature.
- 7. The method according to claim 6, which comprises carrying out a verification of the digital signature.
- 8. The method according to claim 1, which comprises carrying out an asymmetrical authentication.
- 9. In a device for cryptographic processing, a processor unit programmed to:





prescribe an elliptic curve in a first form, with a plurality of first parameters determining the elliptic curve;

transform the elliptic curve into a second form

$$y^2 = x^3 + c^4 ax + c^6 b$$

by determining a plurality of second parameters, at least one of the second parameters being shortened in length by comparison with the first parameter;

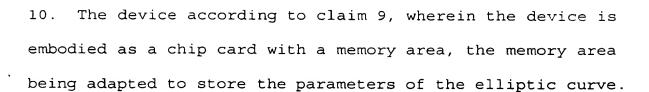
wherein x,y are variables;

- a,b are the first parameters; and
- c is a constant;

shorten the at least the parameter a by selecting the constant c such that

can be determined to be much shorter than the length of the parameter b and the length of the prescribed variable p; and

determine the elliptic curve in the second form for the purpose of cryptographic processing.



- 11. The device according to claim 10, wherein the chip card has a protected memory area adapted to store a secret key.
- 12. A computer-readable medium having computer-executable instructions for performing a cryptographic processing method which comprises the steps of:

prescribing an elliptic curve in a first form, the elliptic curve having a plurality of first parameters;

transforming the elliptic curve into a second form

$$v^2 = x^3 + c^4 a x + c^6 b$$

by determining a plurality of second parameters, wherein at least one of the second parameters is shortened in length by comparison with the first parameter;

wherein x,y are variables;

- a,b are the first parameters; and
- c is a constant;



wherein at least the parameter a is shortened by selecting the constant c such that

c4a mod p

is determined to be significantly shorter than a length of the parameter b and the length of the prescribed variable p; and determining the elliptic curve in the second form for cryptographic processing.

13. The computer-readable medium according to claim 12, wherein the first form of the elliptic curve is defined by  $y^2 = x^3 + ax + b$ .